Attachment E

THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS

PREAMBLE

As the primary criminal investigative agency in the federal government, the Federal Bureau of Investigation (FBI) has the authority and responsibility to investigate all criminal violations of federal law that are not exclusively assigned to another federal agency. The FBI thus plays a central role in the enforcement of federal laws and in the proper administration of justice in the United States. In discharging this function, the highest priority is to protect the security of the nation and the safety of the American people against the depredations of terrorists and foreign aggressors.

Investigations by the FBI are premised upon the fundamental duty of government to protect the public against general crimes, against organized criminal activity, and against those who would threaten the fabric of our society through terrorism or mass destruction. That duty must be performed with care to protect individual rights and to insure that investigations are confined to matters of legitimate law enforcement interest. The purpose of these Guidelines, therefore, is to establish a consistent policy in such matters. The Guidelines will enable Agents of the FBI to perform their duties with greater certainty, confidence and effectiveness, and will provide the American people with a firm assurance that the FBI is acting properly under the law.

These Guidelines provide guidance for general crimes and criminal intelligence investigations by the FBI. The standards and requirements set forth herein govern the circumstances under which such investigations may be begun, and the permissible scope, duration, subject matters, and objectives of these investigations. They do not limit activities carried out under other Attorney General guidelines addressing such matters as investigations and information collection relating to international terrorism, foreign counterintelligence, or foreign intelligence.

The Introduction that follows explains the background of the reissuance of these Guidelines, their general approach and structure, and their specific application in furtherance of the FBI's central mission to protect the United States and its people from acts of terrorism. Part I sets forth general principles that apply to all investigations conducted under these Guidelines. Part II governs investigations undertaken to prevent, solve or prosecute specific violations of federal law. Subpart A of Part III governs criminal intelligence investigations undertaken to obtain information concerning enterprises which are engaged in racketeering activities. Subpart B of Part III governs criminal intelligence investigations undertaken to obtain information concerning enterprises which seek to further political or social goals through violence or which otherwise aim to engage in terrorism or the commission of terrorism-related crimes. Parts IV through VII discuss authorized investigative techniques, dissemination and maintenance of information, counterterrorism activities and other authorized law enforcement activities, and miscellaneous matters.

These Guidelines are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code.

TABLE OF CONTENTS

INTRODUCTION 1

A. CHECKING OF LEADS AND PRELIMINARY INQUIRIES 1

B. FULL INVESTIGATIONS 2

C. AUTHORIZED INVESTIGATIVE TECHNIQUES 6

D. OTHER AUTHORIZED ACTIVITIES 6

I. GENERAL PRINCIPLES 6

II. GENERAL CRIMES INVESTIGATIONS 8

A. DEFINITIONS 8

B. PRELIMINARY INQUIRIES 8

C. INVESTIGATIONS 10

III. CRIMINAL INTELLIGENCE INVESTIGATIONS 12

A. RACKETEERING ENTERPRISE INVESTIGATIONS 13

1. Definition 13

2. General Authority 13

3. Purpose 14

4. Scope 14

5. Authorization and Renewal 14

B. TERRORISM ENTERPRISE INVESTIGATIONS 15

1. General Authority 15

2. Purpose 17

3. Scope 17

4. Authorization and Renewal 17

IV. INVESTIGATIVE TECHNIQUES 18

V. DISSEMINATION AND MAINTENANCE OF INFORMATION 20

VI. COUNTERTERRORISM ACTIVITIES AND OTHER AUTHORIZATIONS . . . 21

A. COUNTERTERRORISM ACTIVITIES 21

1. Information Systems 21

2. Visiting Public Places and Events 22

B. OTHER AUTHORIZATIONS 22

1. General Topical Research 22

2. Use of Online Resources Generally 22

3. Reports and Assessments 23

4. Cooperation with Secret Service 23

C. PROTECTION OF PRIVACY AND OTHER LIMITATIONS 23

1. General Limitations 23

2. Maintenance of Records Under the Privacy Act 23

3. Construction of Part 24

VII. RESERVATION 24

INTRODUCTION

Following the September 11, 2001, terrorist attack on the United States, the Department of Justice carried out a general review of existing guidelines and procedures relating to national security and criminal matters. The reissuance of these Guidelines reflects the result of that review.

These Guidelines follow previous guidelines in their classification of levels of investigative activity, in their classification of types of investigations, in their standards for initiating investigative activity, and in their identification of permitted investigative techniques. There are, however, a number of changes designed to enhance the general effectiveness of criminal investigation, to bring the Guidelines into conformity with recent changes in the law, and to facilitate the FBI's central mission of preventing the commission of terrorist acts against the United States and its people.

In their general structure, these Guidelines provide graduated levels of investigative activity, allowing the FBI the necessary flexibility to act well in advance of the commission of planned terrorist acts or other federal crimes. The three levels of investigative activity are: (1) the prompt and extremely limited checking of initial leads, (2) preliminary inquiries, and (3) full investigations. Subject to these Guidelines and other guidelines and policies noted in Part IV below, any lawful investigative technique may be used in full investigations, and with some exceptions, in preliminary inquiries.

A. CHECKING OF LEADS AND PRELIMINARY INQUIRIES

The lowest level of investigative activity is the "prompt and extremely limited checking out of initial leads," which should be undertaken whenever information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted. This limited activity should be conducted with an eye toward promptly determining whether further investigation (either a preliminary inquiry or a full investigation) should be conducted.

The next level of investigative activity, a preliminary inquiry, should be undertaken when there is information or an allegation which indicates the possibility of criminal activity and whose responsible handling requires some further scrutiny beyond checking initial leads. This authority allows FBI agents to respond to information that is ambiguous or incomplete. Even where the available information meets only this threshold, the range of available investigative techniques is broad. These Guidelines categorically prohibit only mail opening and nonconsensual electronic surveillance at this stage. Other methods, including the development of sources and informants and undercover activities and operations, are permitted in preliminary inquiries. The tools available to develop information sufficient for the commencement of a full investigation, or determining that one is not merited – the purpose of a preliminary inquiry – should be fully employed, consistent with these Guidelines, with a view toward preventing terrorist activities.

Whether it is appropriate to open a preliminary inquiry immediately, or instead to engage first in a limited checking out of leads, depends on the circumstances presented. If, for example, an agent receives an allegation that an individual or group has advocated the commission of criminal violence, and no other facts are available, an appropriate first step would be checking out of leads to determine whether the individual, group, or members of the audience have the apparent ability or intent to carry out the advocated crime. A similar response would be appropriate on the basis of non-verbal conduct of an ambiguous character – for example, where a report is received that an individual has accumulated explosives that could be used either in a legitimate business or to commit a terrorist act. Where the limited checking out of leads discloses a possibility or reasonable indication of criminal activity, a preliminary inquiry or full investigation may then be initiated. However, if the available information shows at the outset that the threshold standard for a preliminary inquiry or full investigation is satisfied, then the appropriate investigative activity may be initiated immediately, without progressing through more limited investigative stages.

The application of these Guidelines' standards for inquiries merits special attention in cases that involve efforts by individuals or groups to obtain, for no apparent reason, biological, chemical, radiological, or nuclear materials whose use or possession is constrained by such statutes as 18 U.S.C. 175, 229, or 831. For example, FBI agents are not required to possess information relating to an individual's intended criminal use of dangerous biological agents or toxins prior to initiating investigative activity. On the contrary, if an individual or group has attempted to obtain such materials, or has indicated a desire to acquire them, and the reason is not apparent, investigative action, such as conducting a checking out of leads or initiating a preliminary inquiry, may be appropriate to determine whether there is a legitimate purpose for the possession of the materials by the individual or group. Likewise, where individuals or groups engage in efforts to acquire or show an interest in acquiring, without apparent reason, toxic chemicals or their precursors or radiological or nuclear materials, investigative action to determine whether there is a legitimate purpose may be justified.

B. FULL INVESTIGATIONS

These Guidelines provide for two types of full investigations: general crimes investigations (Part II below) and criminal intelligence investigations (Part III below). The choice of the type of investigation depends on the information and the investigative focus. A general crimes investigation may be initiated where facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed. Preventing future criminal activity, as well as solving and prosecuting crimes that have already occurred, is an explicitly authorized objective of general crimes investigations. The "reasonable indication" threshold for undertaking such an investigation is substantially lower than probable cause. In addition, preparation to commit a criminal act can itself be a current criminal violation under the conspiracy or attempt provisions of federal criminal law or other provisions defining preparatory crimes, such as 18 U.S.C. 373 (solicitation of a crime of violence) or 18 U.S.C. 2339A (including provision of material support in preparation for a terrorist crime). Under these

Guidelines, a general crimes investigation is warranted where there is not yet a current substantive or preparatory crime, but where facts or circumstances reasonably indicate that such a crime will occur in the future.

The second type of full investigation authorized under these Guidelines is the criminal intelligence investigation. The focus of criminal intelligence investigations is the group or enterprise, rather than just individual participants and specific acts. The immediate purpose of such an investigation is to obtain information concerning the nature and structure of the enterprise – including information relating to the group's membership, finances, geographical dimensions, past and future activities, and goals – with a view toward detecting, preventing, and prosecuting the enterprise's criminal activities. Criminal intelligence investigations, usually of a long-term nature, may provide vital intelligence to help prevent terrorist acts.

Authorized criminal intelligence investigations are of two types: racketeering enterprise investigations (Part III.A) and terrorism enterprise investigations (Part III.B).

A racketeering enterprise investigation may be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in a pattern of racketeering activity as defined in the Racketeer Influenced and Corrupt Organizations Act (RICO). However, the USA PATRIOT ACT (Public Law 107-56) expanded the predicate acts for RICO to include the crimes most likely to be committed by terrorists and their supporters, as described in 18 U.S.C. 2332b(g)(5)(B). To maintain uniformity in the standards and procedures for criminal intelligence investigations relating to terrorism, investigations premised on racketeering activity involving offenses described in 18 U.S.C. 2332b(g)(5)(B) are subject to the provisions for terrorism enterprise investigations rather than those for racketeering enterprise investigations.

A terrorism enterprise investigation may be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of: (1) furthering political or social goals wholly or in part through activities that involve force or violence and a federal crime, (2) engaging in terrorism as defined in 18 U.S.C. 2331(1) or (5) that involves a federal crime, or (3) committing any offense described in 18 U.S.C. 2332b(g)(5)(B). As noted above, criminal intelligence investigations premised on a pattern of racketeering activity involving an 18 U.S.C. 2332b(g)(5)(B) offense are also treated as terrorism enterprise investigations.

As with the other types of full investigations authorized by these Guidelines, any lawful investigative technique may be used in terrorism enterprise investigations, including the development of sources and informants and undercover activities and operations. The "reasonable indication" standard for commencing a terrorism enterprise investigation is the same as that for general crimes and racketeering enterprise investigations. As noted above, it is substantially lower than probable cause.

In practical terms, the "reasonable indication" standard for opening a criminal intelligence investigation of an enterprise in the terrorism context could be satisfied in a number of ways. In some cases satisfaction of the standard will be apparent on the basis of direct evidence of an enterprise's involvement in or planning for the commission of a federal offense involving the use of force or violence to further political or social goals, terrorism as defined in 18 U.S.C. 2331(1) or (5), or a crime described in 18 U.S.C. 2332b(g)(5)(B). For example, direct information may be available about statements made in furtherance of an enterprise's objectives which show a purpose of committing such crimes or securing their commission by others.

In other cases, the nature of the conduct engaged in by an enterprise will justify an inference that the standard is satisfied, even if there are no known statements by participants that advocate or indicate planning for violence or other prohibited acts. For example, such activities as attempting to obtain dangerous biological agents, toxic chemicals, or nuclear materials, or stockpiling explosives or weapons, with no discernible lawful purpose, may be sufficient to reasonably indicate that an enterprise aims to engage in terrorism.

Moreover, a group's activities and the statements of its members may properly be considered in conjunction with each other. A combination of statements and activities may justify a determination that the threshold standard for a terrorism enterprise investigation is satisfied, even if the statements alone or the activities alone would not warrant such a determination.

While no particular factor or combination of factors is required, considerations that will generally be relevant to the determination whether the threshold standard for a terrorism enterprise investigation is satisfied include, as noted, a group's statements, its activities, and the nature of potential federal criminal law violations suggested by its statements or activities. Thus, where there are grounds for inquiry concerning a group, it may be helpful to gather information about these matters, and then to consider whether these factors, either individually or in combination, reasonably indicate that the group is pursuing terrorist activities or objectives as defined in the threshold standard. Findings that would weigh in favor of such a conclusion include, for example, the following:

(1) Threats or advocacy of violence or other covered criminal acts:
Statements are made in relation to or in furtherance of an enterprise's political or social objectives that threaten or advocate the use of force or violence, or statements are made in furtherance of an enterprise that otherwise threaten or advocate criminal conduct within the scope of 18 U.S.C. 2331(1) or (5) or 2332b(g)(5)(B), which may concern such matters as (e.g.):

(i) engaging in attacks involving or threatening massive loss of life or injury, mass destruction, or endangerment of the national security;

(ii) killing or injuring federal personnel, destroying federal facilities, or defying lawful federal authority;

(iii) killing, injuring or intimidating individuals because of their status as United States nationals or persons, or because of their national origin, race, color, religion, or sex; or

(iv) depriving individuals of any rights secured by the Constitution or laws of the United States.

(2) Apparent ability or intent to carry out violence or other covered activities:
The enterprise manifests an apparent ability or intent to carry out violence or other activities within the scope of 18 U.S.C. 2331(1) or (5) or 2332b(g)(5)(B), e.g.:

(i) by acquiring, or taking steps towards acquiring, biological agents or toxins, toxic chemicals or their precursors, radiological or nuclear materials, explosives, or other destructive or dangerous materials (or plans or formulas for such materials), or weapons, under circumstances where, by reason of the quantity or character of the items, the lawful purpose of the acquisition is not apparent;

(ii) by the creation, maintenance, or support of an armed paramilitary organization;

(iii) by paramilitary training; or

(iv) by other conduct demonstrating an apparent ability or intent to injure or intimidate individuals, or to interfere with the exercise of their constitutional or statutory rights.

(3) Potential federal crime:
The group's statements or activities suggest potential federal criminal violations that may be relevant in applying the standard for initiating a terrorism enterprise investigation – such as crimes under the provisions of the U.S. Code that set forth specially defined terrorism or support-of-terrorism offenses, or that relate to such matters as aircraft hijacking or destruction, attacks on transportation, communications, or energy facilities or systems, biological or chemical weapons, nuclear or radiological materials, civil rights violations, assassinations or other violence against federal officials or facilities, or explosives (e.g., the offenses listed in 18 U.S.C. 2332b(g)(5)(B) or appearing in such provisions as 18 U.S.C. 111, 115, 231, 241, 245, or 247).

C. AUTHORIZED INVESTIGATIVE TECHNIQUES

All lawful investigative techniques may be used in general crimes, racketeering enterprise, and terrorism enterprise investigations. In preliminary inquiries, these Guidelines bar the use of mail openings and nonconsensual electronic surveillance (including all techniques covered by chapter 119 of title 18, United States Code), but do not categorically prohibit the use of any other lawful investigative technique at that stage. As set forth in Part IV below, authorized methods in investigations include, among others, use of confidential informants, undercover activities and operations, nonconsensual electronic surveillance, pen registers and trap and trace devices, accessing stored wire and electronic communications and transactional records, consensual electronic monitoring, and searches and seizures. All requirements for the use of such methods under the Constitution, applicable statutes, and Department regulations or policies must, of course, be observed.

D. OTHER AUTHORIZED ACTIVITIES

Current counterterrorism priorities and the advent of the Internet have raised a number of issues which did not exist in any comparable form when the last general revision of these Guidelines was carried out in 1989 – a time long preceding the September 11 attack's disclosure of the full magnitude of the terrorist threat to the United States, and a time in which the Internet was not available in any developed form as a source of information for counterterrorism and other anti-crime purposes. Part VI of these Guidelines is designed to provide clear authorizations and statements of governing principles for a number of important activities that affect these areas. Among other things, Part VI makes it clear that the authorized law enforcement activities of the FBI include: (i) operating and participating in counterterrorism information systems, such as the Foreign Terrorist Tracking Task Force (VI.A(1)); (ii) visiting places and events which are open to the public for the purpose or detecting or preventing terrorist activities (VI.A(2)); (iii) carrying out general topical research, such as searching online under terms like "anthrax" or "smallpox" to obtain publicly available information about agents that may be used in bioterrorism attacks (VI.B(1)); (iv) surfing the Internet as any member of the public might do to identify, e.g., public websites, bulletin boards, and chat rooms in which bomb making instructions, child pornography, or stolen credit card information is openly traded or disseminated, and observing information open to public view in such forums to detect terrorist activities and other criminal activities (VI.B(2)); (v) preparing general reports and assessments relating to terrorism or other criminal activities in support of strategic planning and investigative operations (VI.B(3)); and (vi) providing investigative assistance to the Secret Service in support of its protective responsibilities (VI.B(4)).

I. GENERAL PRINCIPLES

Preliminary inquiries and investigations governed by these Guidelines are conducted for the purpose of preventing, detecting, or prosecuting violations of federal law. The FBI shall

fully utilize the methods authorized by these Guidelines to maximize the realization of these objectives.

The conduct of preliminary inquiries and investigations may present choices between the use of investigative methods which are more or less intrusive, considering such factors as the effect on the privacy of individuals and potential damage to reputation. Inquiries and investigations shall be conducted with as little intrusion as the needs of the situation permit. It is recognized, however, that the choice of techniques is a matter of judgment. The FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the intrusiveness is warranted in light of the seriousness of a crime or the strength of the information indicating its commission or potential future commission. This point is to be particularly observed in the investigation of terrorist crimes and in the investigation of enterprises that engage in terrorism.

All preliminary inquiries shall be conducted pursuant to the General Crimes Guidelines (i.e., Part II of these Guidelines). There is no separate provision for preliminary inquiries under the Criminal Intelligence Guidelines (i.e., Part III of these Guidelines) because preliminary inquiries under Part II may be carried out not only to determine whether the grounds exist to commence a general crimes investigation under Part II, but alternatively or in addition to determine whether the grounds exist to commence a racketeering enterprise investigation or terrorism enterprise investigation under Part III. A preliminary inquiry shall be promptly terminated when it becomes apparent that a full investigation is not warranted. If, on the basis of information discovered in the course of a preliminary inquiry, an investigation is warranted, it may be conducted as a general crimes investigation, or a criminal intelligence investigation, or both. All such investigations, however, shall be based on a reasonable factual predicate and shall have a valid law enforcement purpose.

In its efforts to anticipate or prevent crime, the FBI must at times initiate investigations in advance of criminal conduct. It is important that such investigations not be based solely on activities protected by the First Amendment or on the lawful exercise of any other rights secured by the Constitution or laws of the United States. When, however, statements advocate criminal activity or indicate an apparent intent to engage in crime, particularly crimes of violence, an investigation under these Guidelines may be warranted unless it is apparent, from the circumstances or the context in which the statements are made, that there is no prospect of harm.

General crimes investigations and criminal intelligence investigations shall be terminated when all logical leads have been exhausted and no legitimate law enforcement interest justifies their continuance.

Nothing in these Guidelines prohibits the FBI from ascertaining the general scope and nature of criminal activity in a particular location or sector of the economy, or from collecting and maintaining publicly available information consistent with the Privacy Act.

II. GENERAL CRIMES INVESTIGATIONS

A. DEFINITIONS

(1) "Exigent circumstances" are circumstances requiring action before authorization otherwise necessary under these guidelines can reasonably be obtained, in order to protect life or substantial property interests; to apprehend or identify a fleeing offender; to prevent the hiding, destruction or alteration of evidence; or to avoid other serious impairment or hindrance of an investigation.

(2) "Sensitive criminal matter" is any alleged criminal conduct involving corrupt action by a public official or political candidate, the activities of a foreign government, the activities of a religious organization or a primarily political organization or the related activities of any individual prominent in such an organization, or the activities of the news media; and any other matter which in the judgment of a Special Agent in Charge (SAC) should be brought to the attention of the United States Attorney or other appropriate official in the Department of Justice, as well as FBI Headquarters (FBIHQ).

B. PRELIMINARY INQUIRIES

(1) On some occasions the FBI may receive information or an allegation not warranting a full investigation -- because there is not yet a "reasonable indication" of criminal activities – but whose responsible handling requires some further scrutiny beyond the prompt and extremely limited checking out of initial leads. In such circumstances, though the factual predicate for an investigation has not been met, the FBI may initiate an "inquiry" in response to the allegation or information indicating the possibility of criminal activity.

This authority to conduct inquiries short of a full investigation allows the government to respond in a measured way to ambiguous or incomplete information, with as little intrusion as the needs of the situation permit. This is especially important in such areas as white-collar crime where no complainant is involved or when an allegation or information is received from a source of unknown reliability. Such inquiries are subject to the limitations on duration under paragraph (3) below and are carried out to obtain the information necessary to make an informed judgment as to whether a full investigation is warranted.

A preliminary inquiry is not a required step when facts or circumstances reasonably indicating criminal activity are already available; in such cases, a full investigation can be immediately opened.

(2) The FBI supervisor authorizing an inquiry shall assure that the allegation or other information which warranted the inquiry has been recorded in writing. In sensitive

criminal matters, the United States Attorney or an appropriate Department of Justice official shall be notified of the basis for an inquiry as soon as practicable after the opening of the inquiry, and the fact of notification shall be recorded in writing.

(3) Inquiries shall be completed within 180 days after initiation of the first investigative step. The date of the first investigative step is not necessarily the same date on which the first incoming information or allegation was received. An extension of time in an inquiry for succeeding 90-day periods may be granted. A SAC may grant up to two extensions based on a statement of the reasons why further investigative steps are warranted when there is no "reasonable indication" of criminal activity. All extensions following the second extension may only be granted by FBI Headquarters upon receipt of a written request and such a statement of reasons.

(4) The choice of investigative techniques in an inquiry is a matter of judgment, which should take account of: (i) the objectives of the inquiry and available investigative resources, (ii) the intrusiveness of a technique, considering such factors as the effect on the privacy of individuals and potential damage to reputation, (iii) the seriousness of the possible crime, and (iv) the strength of the information indicating its existence or future commission. Where the conduct of an inquiry presents a choice between the use of more or less intrusive methods, the FBI should consider whether the information could be obtained in a timely and effective way by the less intrusive means. The FBI should not hesitate to use any lawful techniques consistent with these Guidelines in an inquiry, even if intrusive, where the intrusiveness is warranted in light of the seriousness of the possible crime or the strength of the information indicating its existence or future commission. This point is to be particularly observed in inquiries relating to possible terrorist activities.

(5) All lawful investigative techniques may be used in an inquiry except:

(a) Mail openings; and

(b) Nonconsensual electronic surveillance or any other investigative technique covered by chapter 119 of title 18, United States Code (18 U.S.C. 2510-2522).

(6) The following investigative techniques may be used in an inquiry without any prior authorization from a supervisory agent:

(a) Examination of FBI indices and files;

(b) Examination of records available to the public and other public sources of information;

dissemination and use of FISA – acquired information. Recognizing the broad sweep of acquisition allowed under FISA's definition of electronic surveillance (and, subsequently, physical searches), coupled with the low threshold for retention in the "could not be foreign intelligence" standard, Congress has provided guidance for the Court in the FISA's legislative history:

> On the other hand, given this degree of latitude the committee believes it is imperative that with respect to information concerning U.S. persons which is retained as necessary for counterintelligence or counter terrorism purposes, rigorous and strict controls be placed on the retrieval of such identifiable information and its dissemination or use for purposes other than counterintelligence or counter terrorism. (emphasis added)[5]

> The judge has the discretionary power to modify the order sought, such as with regard to the period of authorization . . . or the minimization procedures to be followed. (emphasis added)[6]The Committee contemplates that the court would give these procedures most careful consideration. If it is not of the opinion that they will be effective, the procedures should be modified. (emphasis added)[7]

Between 1979 when the FISA became operational and 1995, the government relied on the standard minimization procedures described herein to regulate all electronic surveillances. In 1995, following amendment of the FISA to permit physical searches, comparable minimization procedures were adopted for foreign intelligence searches. On July 19, 1995, the Attorney General issued Procedures for Contacts Between the FBI and Criminal Division Concerning FI and Foreign Counterintelligence Investigations, which in part A regulated "Contacts During an FI

---

[5] Id. at 59.

[6] Id at 78.

[7] Id. at 80.

or FCI Investigation in Which FISA Surveillance or Searches are Being Conducted" between FBI personnel and trial attorneys of the Department's Criminal Division. The Court was duly informed of these procedures and has considered them an integral part of the minimization process although they were not formally submitted to the Court under §1804 (a)(5) or §1823(a)(5). In January, 2000 the Attorney General augmented the 1995 procedures to permit more information sharing from FISA cases with the Criminal Division, and the current Deputy Attorney General expanded the procedures in August 2001. Taken together, the 1995 procedures, as augmented, permit substantial consultation and coordination as follows:

a. reasonable indications of significant federal crimes in FISA cases are to be reported to the Criminal Division of the Department of Justice;

b. The Criminal Division may then consult with the FBI and give guidance to the FBI aimed at preserving the option of criminal prosecution, but may not direct or control the FISA investigation toward law enforcement objectives;

c. the Criminal Division may consult further with the appropriate U.S. Attorney's Office about such FISA cases;

d. on a monthly basis senior officials of the FBI provide briefings to senior officials of the Justice Department, including OIPR and the Criminal Division, about intelligence cases, including those in which FISA is or may be used;

e. all FBI 90-day interim reports and annual reports of counterintelligence investigations, including FISA cases, are being provided to the Criminal Division, and must now contain a section explicitly identifying any possible federal criminal violations;

f. all requests for initiation or renewal of FISA authority must now contain a section devoted explicitly to identifying any possible federal criminal violations;

g. the FBI is to provide monthly briefings directly to the Criminal Division

concerning all counterintelligence investigations in which there is a reasonable indication of a significant federal crime;

h. prior to each briefing the Criminal Division is to identify (from FBI reports) those intelligence investigations about which it requires additional information and the FBI is to provide the information requested; and

i. since September 11, 2001, the requirement that OIPR be present at all meetings and discussions between the FBI and Criminal Division involving certain FISA cases has been suspended; instead, OIPR reviews a daily briefing book to inform itself and this Court about those discussions.

The Court came to rely on these supplementary procedures, and approved their broad information sharing and coordination with the Criminal Division in thousands of applications. In addition, because of the FISA's requirement (since amended) that the FBI Director certify that "the purpose" of each surveillance and search was to collect foreign intelligence information, the Court was routinely apprised of consultations and discussions between the FBI, the Criminal Division, and U.S. Attorney's offices in cases where there were overlapping intelligence and criminal investigations or interests. This process increased dramatically in numerous FISA applications concerning the September 11th attack on the World Trade Center and the Pentagon.

In order to preserve both the appearance and the fact that FISA surveillances and searches were not being used sub rosa for criminal investigations, the Court routinely approved the use of information screening "walls" proposed by the government in its applications. Under the normal "wall" procedures, where there were separate intelligence and criminal investigations, or a single counter-espionage investigation with overlapping intelligence and criminal interests, FBI criminal investigators and Department prosecutors were not allowed to review all of the raw FISA

intercepts or seized materials lest they become defacto partners in the FISA surveillances and searches. Instead, a screening mechanism, or person, usually the chief legal counsel in an FBI field office, or an assistant U.S. attorney not involved in the overlapping criminal investigation, would review all of the raw intercepts and seized materials and pass on only that information which might be relevant evidence. In unusual cases such as where attorney-client intercepts occurred, Justice Department lawyers in OIPR acted as the "wall." In significant cases, involving major complex investigations such as the bombings of the U.S. Embassies in Africa, and the millennium investigations, where criminal investigations of FISA targets were being conducted concurrently, and prosecution was likely, this Court became the "wall" so that FISA information could not be disseminated to criminal prosecutors without the Court's approval. In some cases where this Court was the "wall," the procedures seemed to have functioned as provided in the Court's orders; however, in an alarming number of instances, there have been troubling results.

Beginning in March 2000, the government notified the Court that there had been disseminations of FISA information to criminal squads in the FBI's New York field office, and to the U.S. Attorney's Office for the Southern District of New York, without the required authorization of the Court as the "wall" in four or five FISA cases. Subsequently, the government filed a notice with the Court about it's unauthorized disseminations.

In September 2000, the government came forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts, including:

a. an erroneous statement in the FBI Director's FISA certification that the target of the FISA was not under criminal investigation;

b. erroneous statements in the FISA affidavits of FBI agents concerning the separation of the overlapping intelligence and criminal investigations, and the unauthorized sharing of FISA information with FBI criminal investigators and assistant U.S. attorneys;

c. omissions of material facts from FBI FISA affidavits relating to a prior relationship between the FBI and a FISA target, and the interview of a FISA target by an assistant U.S. attorney.

In November of 2000, the Court held a special meeting to consider the troubling number of inaccurate FBI affidavits in so many FISA applications. After receiving a more detailed explanation from the Department of Justice about what went wrong, but not why , the Court decided not to accept inaccurate affidavits from FBI agents whether or not intentionally false. One FBI agent was barred from appearing before the Court as a FISA affiant. The Court decided to await the results of the investigation by the Justice Department's Office of Professional Responsibility before taking further action.

In March of 2001, the government reported similar misstatements in another series of FISA applications in which there was supposedly a "wall" between separate intelligence and criminal squads in FBI field offices to screen FISA intercepts, when in fact all of the FBI agents were on the same squad and all of the screening was done by the one supervisor overseeing both investigations.

To come to grips with this problem, in April of 2001, the FBI promulgated detailed procedures governing the submission of requests to conduct FISA surveillances and searches, and to review draft affidavits in FISA applications, to ensure their accuracy. These procedures are

currently in use and require careful review of draft affidavits by the FBI agents in the field offices who are conducting the FISA case investigations, as well as the supervising agents at FBI headquarters who appear before the Court and swear to the affidavits.

In virtually every instance, the government's misstatements and omissions in FISA applications and violations of the Court's orders involved information sharing and unauthorized disseminations to criminal investigators and prosecutors. These incidents have been under investigation by the FBI's and the Justice Department's Offices of Professional Responsibility for more than one year to determine how the violations occurred in the field offices, and how the misinformation found its way into the FISA applications and remained uncorrected for more than one year despite procedures to verify the accuracy of FISA pleadings. As of this date, no report has been published, and how these misrepresentations occurred remains unexplained to the Court.

As a consequence of the violations of its orders, the Court has taken some supervisory actions to assess compliance with the "wall" procedures. First, until September 15, 2001 it required all Justice Department personnel who received certain FISA information to certify that they understood that under "wall" procedures FISA information was not to be shared with criminal prosecutors without the Court's approval. Since then, the Court has authorized criminal division trial attorneys to review all FBI international terrorism case files, including FISA case files and required reports from FBI personnel and Criminal Division attorneys describing their discussions of the FISA cases. The government's motion that the Court rescind all "wall" procedures in all international terrorism surveillances and searches now pending before the Court,

or that has been before the Court at any time in the past, was deferred by the Court until now, at the suggestion of the government, pending resolution of this matter.

Given this history in FISA information sharing, the Court now turns to the revised 2002 minimization procedures. We recite this history to make clear that the Court has long approved, under controlled circumstances, the sharing of FISA information with criminal prosecutors, as well as consultations between intelligence and criminal investigations where FISA surveillances and searches are being conducted. However, the proposed 2002 minimization procedures eliminate the bright line in the 1995 procedures prohibiting direction and control by prosecutors on which the Court has relied to moderate the broad acquisition retention, and dissemination of FISA information in overlapping intelligence and criminal investigations. Paragraph A.6. of the1995 procedures provided in part:

> Additionally, the FBI and the Criminal Division should ensure that advice intended to preserve the option of a criminal prosecution does not inadvertently result in either the fact or the appearance of the Criminal Division's directing or controlling the FI or FCI investigation toward law enforcement objectives. (emphasis added)

As we conclude the first part of our statutory task, we have determined that the extensive acquisition of information concerning U.S. persons through secretive surveillances and searches authorized under FISA, coupled with broad powers of retention and information sharing with criminal prosecutors, weigh heavily on one side of the scale which we must balance to ensure that the proposed minimization procedures are "consistent" with the need of the United States to obtain, produce, and disseminate foreign intelligence information. (§1805(a)(4) and §1824)(a)(4))

III

The 2002 minimization rules set out in sections II and III, "Intelligence Sharing Procedures Concerning the Criminal Division" and "Intelligence Sharing Procedures Concerning a USAO," continue the existing practice approved by this Court of in-depth dissemination of FISA information to Criminal Division trial attorneys and U.S. Attorney's Offices (hereafter criminal prosecutors). These new procedures apply in two kinds of counterintelligence cases in which FISA is the only effective tool available to both counterintelligence and criminal investigators:

1) those cases in which separate intelligence and criminal investigations of the same U.S. person FISA target are conducted by different FBI agents (overlapping investigations), usually involving international terrorism, and in which separation can easily be maintained, and

2) those cases in which one investigation having a U.S. person FISA target is conducted by a team of FBI agents which has both intelligence and criminal interests (overlapping interests) usually involving espionage and similar crimes in which separation is impractical.

In both kinds of counterintelligence investigations where FISA is being used, the proposed 2002 minimization procedures authorize extensive consultations between the FBI and criminal prosecutors "to coordinate efforts to investigate or protect against" actual or potential attack, sabotage, international terrorism and clandestine intelligence activities by foreign powers and their agents as now expressly provided in §1806(k)(1) and §1825(k)(1). These consultations propose to include:

II. A. "Disseminating Information," which gives criminal prosecutors access to "all information developed" in FBI counterintelligence investigations, including FISA acquired information, as well as annual and other reports, and presumably ad hoc reporting of significant events (e.g., incriminating FISA intercepts or seizures) to criminal prosecutors.

II. B. "Providing Advice," where criminal prosecutors are authorized to consult extensively and provide advice and recommendations to intelligence officials about "all issues necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities." Recommendations may include advice about criminal investigation and prosecution as well as the strategy and goals for investigations, the law enforcement and intelligence methods to be used in investigations, and the interaction between intelligence and law enforcement components of investigations.

Last, but most relevant to this Court's finding, criminal prosecutors are empowered to advise FBI intelligence officials concerning "the initiation, operation, continuation, or expansion of FISA searches or surveillance." (emphasis added) This provision is designed to use this Court's orders to enhance criminal investigation and prosecution, consistent with the government's interpretation of the recent amendments that FISA may now be "used primarily for a law enforcement purpose."

In section III," Intelligence Sharing Procedures Concerning a USAO," U.S. attorneys are empowered to "engage in consultations to the same extent as the Criminal Division under parts II. A and II. B of these procedures," in cases involving international terrorism.

A fair reading of these provisions leaves only one conclusion -- under sections II and III of the 2002 minimization procedures, criminal prosecutors are to have a significant role directing FISA surveillances and searches from start to finish in counterintelligence cases having overlapping intelligence and criminal investigations or interests, guiding them to criminal prosecution. The government makes no secret of this policy, asserting its interpretation of the Act's new amendments which "allows FISA to be used primarily for a law enforcement purpose."

Given our experience in FISA surveillances and searches, we find that these provisions in sections II.B and III, particularly those which authorize criminal prosecutors to advise FBI intelligence officials on the initiation, operation, continuation or expansion of FISA's intrusive seizures, are designed to enhance the acquisition, retention and dissemination of evidence for law enforcement purposes, instead of being consistent with the need of the United States to "obtain, produce, and disseminate foreign intelligence information" (emphasis added) as mandated in §1801(h) and §1821(4). The 2002 procedures appear to be designed to amend the law and substitute the FISA for Title III electronic surveillances and Rule 41 searches. This may be because the government is unable to meet the substantive requirements of these law enforcement tools, or because their administrative burdens are too onerous. In either case, the FISA's definition of minimization procedures has not changed, and these procedures cannot be used by the government to amend the Act in ways Congress has not. We also find the provisions in section II.B and III. wanting because the prohibition in the 1995 procedures of criminal

prosecutors "directing or controlling" FISA cases has been revoked by the proposed 2002 procedures. The government's memorandum of law expends considerable effort justifying deletion of that bright line, but the Court is not persuaded.

The Court has long accepted and approved minimization procedures authorizing in-depth information sharing and coordination with criminal prosecutors as described in detail above. In the Court's view, the plain meaning of consultations and coordination now specifically authorized in the Act is based on the need to adjust or bring into alignment two different but complementary interests – intelligence gathering and law enforcement. . In FISA cases this presupposes separate intelligence and criminal investigations, or a single investigation with intertwined interests, which need to be brought into harmony to avoid dysfunction and frustration of either interest. If criminal prosecutors direct both the intelligence and criminal investigations, or a single investigation having combined interests, coordination becomes subordination of both investigations or interests to law enforcement objectives. The proposed 2002 minimization procedures require the Court to balance the government's use of FISA surveillances and searches against the government's need to obtain and use evidence for criminal prosecution, instead of determining the "need of the United States to obtain, produce, and disseminate foreign intelligence information" as mandated by §1801(h) and §1821(4).

Advising FBI intelligence officials on the initiation, operation, continuation or expansion of FISA surveillances and searches of U.S. persons means that criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic

surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute. The 2002 minimization procedures give the Department's criminal prosecutors every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information, including:

- a foreign intelligence standard instead of a criminal standard of probable cause;
- use of the most advanced and highly intrusive techniques for intelligence gathering; and
- surveillances and searches for extensive periods of time;

based on a standard that the U.S. person is only using or about to use the places to be surveilled and searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants. All of this may be done by use of procedures intended to minimize collection of U.S. person information, consistent with the need of the United States to obtain and produce foreign intelligence information. If direction of counterintelligence cases involving the use of highly intrusive FISA surveillances and searches by criminal prosecutors is necessary to obtain and produce foreign intelligence information, it is yet to be explained to the Court.

THEREFORE, because

- the procedures implemented by the Attorney General govern the minimization of electronic surveillances and searches of U.S. persons;
- such intelligence and criminal investigations both target the same U.S. person;

- the information collected through FISA surveillances and searches is both foreign intelligence information and evidence of crime, depending upon who is using it;

- there are pervasive and invasive techniques for electronic surveillances and physical searches authorized under the FISA;

- surveillances and searches may be authorized for extensive periods of time;

- notice of surveillances and searches is not given to the targets unless they are prosecuted;

- the provisions in FISA constrain discovery and adversary hearings and require ex parte, in camera review of FISA surveillances and searches at criminal trial;

- the FISA, as opposed to Title III and Rule 41 searches, is the only tool readily available in these overlapping intelligence and criminal investigation;

- there are extensive provisions in the minimization procedures for dissemination of FISA intercepts and seizures to criminal prosecutors and for consultation and coordination with intelligence officials using the FISA;

- criminal prosecutors would, under the proposed procedures, no longer be prohibited from "directing or controlling" counterintelligence investigations involving use of the FISA toward law enforcement objectives; and

- criminal prosecutors would, under the proposed procedures, be empowered to direct the use of FISA surveillances and searches toward law enforcement objectives by advising FBI intelligence officials on the initiation, operation, continuation and expansion of FISA authority from this Court,

The Court FINDS that parts of section II.B of the minimization procedures submitted with the Government's motion are NOT reasonably designed, in light of their purpose and technique, "consistent with the need of the United States to obtain, produce, or disseminate foreign intelligence information" as defined in §1801(h) and §1821(4) of the Act.

THEREFORE, pursuant to this Court's authority under §1805(a) and §1824(a) to issue ex parte orders for electronic surveillances and physical searches "as requested or as modified," the Court herewith grants the Governments motion BUT MODIFIES the pertinent provisions of sections II. B. of the proposed minimization procedures as follows:

The second and third paragraphs of section II.B shall be deleted, and the following paragraphs substituted in place thereof:

"The FBI, the Criminal Division, and OIPR may consult with each other to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism or clandestine intelligence activities by foreign powers or their agents. Such consultations and coordination may address, among other things, exchanging information already acquired, identifying categories of information needed and being sought, preventing either investigation or interest from obstructing or hindering the other, compromise of either investigation, and long term objectives and overall strategy of both investigations in order to ensure that the overlapping intelligence and criminal interests of the United States are both achieved. Such consultations and coordination may be conducted directly between the components, however, OIPR shall be invited to all such consultations, and if they are unable to attend, OIPR shall be apprised of the substance of the consultations forthwith in writing so that the Court may be notified at the earliest opportunity."

"Notwithstanding the foregoing, law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or

expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives."

These modifications are intended to bring the minimization procedures into accord with the language used in the FISA, and reinstate the bright line used in the 1995 procedures, on which the Court has relied. The purpose of minimization procedures as defined in the Act, is not to amend the statute, but to protect the privacy of Americans in these highly intrusive surveillances and searches, "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

A separate order shall issue this date.

All seven judges of the Court concur in the Corrected and Amended Memorandum Opinion.

Royce C. Lamberth

ROYCE C. LAMBERTH
Presiding Judge

DATE: 5-17-02
6:40 p.m.